

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-237810

(43)Date of publication of application : 23.08.2002

(51)Int.Cl.

H04L 9/08
G06F 17/60

(21)Application number : 2001-035030

(71)Applicant : NEC CORP

(22)Date of filing : 13.02.2001

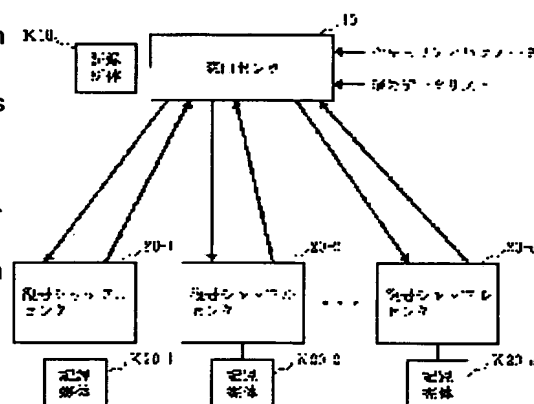
(72)Inventor : SAKO KAZUE
MORI KENGO

(54) ANONYMOUS DECODING SYSTEM, ANONYMOUS DECODING METHOD, AND PROGRAM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To enable an anonymous decoding system to be easily controlled and its initial setting operation to be surely and easily carried out.

SOLUTION: A window center 10 sends security parameters and common public information formed on the basis of the security parameters to decoding shuffle centers 20-1 to 20-m, and the decoding shuffle centers 20-1 to 20-m produce public keys and decoding keys and send back the public keys to the window center 10. The window center 10 synthesizes the received public keys, produces and publicizes encrypting public keys. The window center 10 transfers the encrypted data list to the decoding the j-th shuffle center 20-j when an encrypted data list is decoded, then the window center 10 changes a processing sequence and transfers the received partially decoded data list to the decoding shuffle center 20-(j+1), and the above process is repeatedly carried out. These processes are carried out until the data list is transferred to the last decoding shuffle center 20-m, and the data list sent from the decoding shuffle center 20-m is made to serve as a decoding result.



LEGAL STATUS

[Date of request for examination]

12.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-237810
(P2002-237810A)

(43)公開日 平成14年8月23日(2002.8.23)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 9/08		G 0 6 F 17/60	1 4 8 5 J 1 0 4
G 0 6 F 17/60	1 4 8		5 1 2
	5 1 2	H 0 4 L 9/00	6 0 1 C
			6 0 1 F

審査請求 未請求 請求項の数68 O L (全 18 頁)

(21)出願番号 特願2001-35030(P2001-35030)

(22)出願日 平成13年2月13日(2001.2.13)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 佐古 和恵

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 森 健吾

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100088959

弁理士 境 廣巳

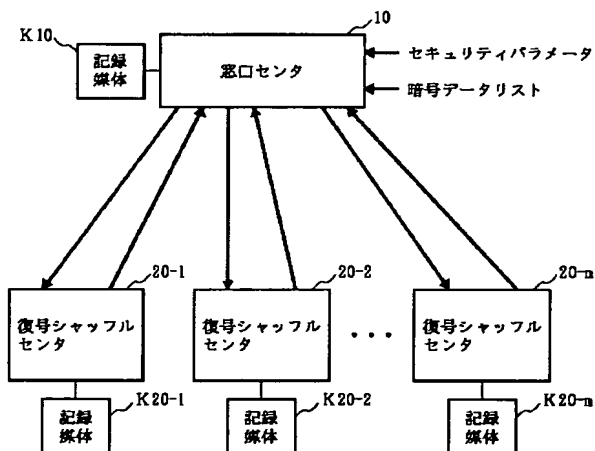
Fターム(参考) 5J104 AA16 EA04 EA24 JA21 PA17

(54)【発明の名称】 匿名復号システム及び匿名復号方法並びにプログラム

(57)【要約】

【課題】 匿名復号システムの管理を容易にすると共に、初期設定操作を容易且つ確実に行えるようにする。

【解決手段】 窓口センタ10は、セキュリティパラメータとそれに基づいて生成した共通公開情報を各復号シャッフルセンタ20-1~20-mへ送り、各復号シャッフルセンタ20-1~20-mは、公開鍵、復号鍵を生成し、公開鍵を窓口センタ10へ返送する。窓口センタ10は、返送された各公開鍵を合成して暗号化用公開鍵を生成し、公開する。また、窓口センタ10は、暗号データリストの復号時、処理順序が第j番目の復号シャッフルセンタ20-jに暗号データリストを転送し、返送されてきた順番入れ替え、部分復号処理の済んだデータリストを次の復号シャッフルセンタ20-(j+1)へ転送するという処理を繰り返し行う。このような処理を最後の復号シャッフルセンタ20-mまで行い、そこから返送されたデータリストを復号結果とする。



【特許請求の範囲】

【請求項1】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタへ転送し、前記復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する窓口センタと、

該窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送する復号シャッフルセンタとを備えたことを特徴とする匿名復号システム。

【請求項2】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

暗号データリストを外部から受け取る窓口センタと、それぞれが復号鍵を所有する複数の復号シャッフルセンタとから成立し、

前記窓口センタは、受け取った暗号データリストを第1の復号シャッフルセンタに転送し、

前記第1の復号シャッフルセンタは、前記窓口センタから受け取った暗号データリストに対して、対応する公開情報を用いて順番入れ替え処理を行い、対応する復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタに返送し、

前記窓口センタは、前記第1の復号シャッフルセンタから返送されたデータリストを、第2の復号シャッフルセンタに送信し、

前記窓口センタは、最後の復号シャッフルセンタから返送されたデータリストを、復号結果リストとして出力することを特徴とする匿名復号システム。

【請求項3】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

窓口センタと、それぞれが復号鍵を所有する複数の復号シャッフルセンタとを備え、

前記窓口センタが、外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第1番目の復号シャッフルセンタへ転送し、処理順序が最後の復号シャッフルセンタ以外の復号シャッフルセンタからデータリストが返送され

てきた場合、処理順序が前記データリストの返送元復号シャッフルセンタの次の復号シャッフルセンタに対して前記返送されてきたデータリストを暗号データリストとして転送し、処理順序が最後の復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する構成を有し、

前記各復号シャッフルセンタが、

前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送する構成を有することを特徴とする匿名復号システム。

【請求項4】 請求項1、2または3記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記窓口センタに報告する構成を有することを特徴とする匿名復号システム。

【請求項5】 請求項1、2または3記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記処理結果のデータリストに付して前記窓口センタに報告する構成を有することを特徴とする匿名復号システム。

【請求項6】 請求項4または5記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証する構成を有することを特徴とする匿名復号システム。

【請求項7】 請求項4または5記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証した後、前記復号シャッフルセンタから返送されてきたデータリストを暗号データリストとして、処理順序が次の復号シャッフルセンタに転送する構成を有することを特徴とする匿名復号システム。

【請求項8】 請求項4、5、6または7記載の匿名復号システムにおいて、

前記窓口センタは、前記復号結果リストに、全復号シャッフルセンタから報告された証明を添付して出力する構成を有することを特徴とする匿名復号システム。

【請求項9】 請求項1、2または3記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行う構成を有することを特徴とする匿名復号システム。

【請求項10】 請求項1、2または3記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付与する構成を有することを特徴とする匿名復号システム。

【請求項11】 請求項1、2または3記載の匿名復号システムにおいて、

同一処理対象に対する、互いに関連する公開情報、暗号データリスト、復号シャッフルセンタが所有する復号鍵に共通のセッションIDを付与し、

前記窓口センタは、或るセッションIDに対応する暗号データリストを復号シャッフルセンタへ転送する場合および復号シャッフルセンタから返送されてきた或るセッションIDの付与されたデータリストを暗号データリストとして復号シャッフルセンタへ転送する場合、前記暗号データリストに前記或るセッションIDを付与して復号シャッフルセンタへ転送する構成を有し、

前記復号シャッフルセンタは、前記窓口センタから或るセッションIDの付与された暗号データリストが転送されてきた場合、前記或るセッションIDの付与されている公開情報を用いて順番入れ替え処理を行い、前記或るセッションIDの付与されている復号鍵を用いて部分復号を行い、その結果のデータリストに前記或るセッションIDを付与して前記窓口センタに返送する構成を有することを特徴とする匿名復号システム。

【請求項12】 請求項1、2または3記載の匿名復号システムにおいて、

前記窓口センタが、セキュリティパラメータが入力されたとき、該セキュリティパラメータに基づいて共通公開情報を作成し、該作成した共通公開情報を全復号シャッフルセンタへ通知し、全復号シャッフルセンタから公開鍵が返送されてきたとき、全復号シャッフルセンタからの公開鍵に基づいて暗号化用公開鍵を生成すると共に、該生成した暗号化用公開鍵と前記共通公開情報とを含んだ公開情報を公開する構成を有し、

前記復号シャッフルセンタが、前記窓口センタから通知された共通公開情報に基づいて、公開鍵および復号鍵を生成し、前記生成した公開鍵を前記窓口センタへ返送する構成を有することを特徴とする匿名復号システム。

【請求項13】 請求項12記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、公開鍵を前記窓口センタへ返送するとき、正しく前記公開鍵を生成したことの証明を付して前記窓口センタに返送する構成を有することを特徴とする匿名復号システム。

【請求項14】 請求項13記載の匿名復号システムにおいて、

前記窓口センタは、公開鍵に付された証明が正しいことを検証する構成を有することを特徴とする匿名復号システム。

【請求項15】 請求項13または14記載の匿名復号システムにおいて、

前記窓口センタは、公開鍵と、公開鍵に付与された証明を公開情報とともに公開する構成を有することを特徴とする匿名復号システム。

【請求項16】 請求項12記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行う構成を有することを特徴とする匿名復号システム。

【請求項17】 請求項12記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信者のデジタル署名を付与する構成を有することを特徴とする匿名復号システム。

【請求項18】 請求項11記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタに対して暗号データリストを転送する際、前記セッションIDに加えて、自窓口センタに付与されている窓口センタID、転送先の復号シャッフルセンタに付与されている復号シャッフルセンタID及び自窓口センタの署名も付加する構成を有することを特徴とする匿名復号システム。

【請求項19】 請求項11記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、前記セッションIDに加えて、自復号シャッフルセンタに付与されている復号シャッフルセンタID、前記窓口センタに付与されている窓口センタID及び自復号シャッフルセンタの署名も付加する構成を有することを特徴とする匿名復号システム。

【請求項20】 請求項19記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、正しく順番入れ替え処理を行ったことの証明データ及び正しく部分復号処理を行ったことの証明データも付加する構成を有することを特徴とする匿名復号システム。

【請求項21】 請求項8記載の匿名復号システムにおいて、

前記窓口センタが出力する情報が、自窓口センタに付与されている窓口センタID、外部から入力した暗号データリスト、該暗号データリストに対する復号結果リスト、前記暗号データリストに付与されているセッションID、全復号シャッフルセンタから返送されてきた全データ及び窓口センタの署名を含むことを特徴とする匿名復号システム。

【請求項22】 請求項12記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタに対して共通

公開情報およびセキュリティパラメータを通知する際、自窓口センタに付与されている窓口センタID、復号を行う全復号シャッフルセンタの復号シャッフルセンタID、セッションID及び窓口センタの署名を付加する構成を有することを特徴とする匿名復号システム。

【請求項23】 請求項12または13記載の匿名復号システムにおいて、復号シャッフルセンタは、窓口センタに返信する情報に、前記窓口センタに付与されている窓口センタID、セッションID、自復号シャッフルセンタの復号シャッフルセンタID及び自復号シャッフルセンタの署名を付加する構成を有することを特徴とする匿名復号システム。

【請求項24】 請求項12記載の匿名復号システムにおいて、前記窓口センタが公開する公開情報は、自窓口センタに付与されている窓口センタID、セッションID、セキュリティパラメータ、暗号化用公開鍵、全復号シャッフルセンタの復号シャッフルセンタID及び全復号シャッフルセンタが生成した公開鍵を含むことを特徴とする匿名復号システム。

【請求項25】 請求項4、5、9または13記載の匿名復号システムにおいて、復号シャッフルセンタが行った証明は、第三者により検証できるものであることを特徴とする匿名復号システム。

【請求項26】 請求項1、2または3記載の匿名復号システムにおいて、前記復号シャッフルセンタは、順番入れ替え処理に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前計算したデータを用いて順番入れ替え処理を行う構成を有することを特徴とする匿名復号システム。

【請求項27】 請求項5記載の匿名復号システムにおいて、前記復号シャッフルセンタは、順番入れ替え処理が正しいことを証明する証明データの生成に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前に計算したデータを用いて前記証明データを生成する構成を有することを特徴とする匿名復号システム。

【請求項28】 請求項1乃至27記載の何れか1つの匿名復号システムにおいて、各投票者から送られてくる、投票データを前記公開情報に基づいて暗号化した暗号化投票データを受け付け、その中から正当な投票者の正当な暗号化投票データを選別し、該選別した暗号化投票データを暗号データリストとして前記窓口センタに送信する投票管理センタを備えたことを特徴とする匿名復号システム。

【請求項29】 請求項28記載の匿名復号システムにおいて、前記各投票者は、正しく投票データを暗号化したことを

証明する証明データを前記投票管理センタへ送信し、前記投票管理センタは、各投票者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

【請求項30】 請求項1乃至27記載の何れか1つの匿名復号システムにおいて、

各入札者から送られてくる、入札値を前記公開情報に基づいて暗号化した暗号化入札値を受け付け、その中から正当な入札者の正当な暗号化入札値を選別し、該選別した暗号化入札値を暗号化データリストとして前記窓口センタへ送信する入札管理センタを備えたことを特徴とする匿名復号システム。

【請求項31】 請求項30記載の匿名復号システムにおいて、

前記各入札者は、正しく入札値を暗号化したことを証明する証明データを前記入札管理センタへ送信し、前記入札管理センタは、各入札者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

20 【請求項32】 請求項1乃至請求項27記載の何れか1つの匿名復号システムにおいて、

各アンケート回答者から送られてくる、アンケート回答を前記公開情報に基づいて暗号化した暗号化アンケート回答を受け付け、その中から正当なアンケート回答者の正当な暗号化アンケート回答を選別し、該選別した暗号化アンケート回答を暗号化データリストとして前記窓口センタへ送信する受付センタを備えたことを特徴とする匿名復号システム。

30 【請求項33】 請求項32記載の匿名復号システムにおいて、

前記アンケート回答者は、正しくアンケート回答を暗号化したことを証明する証明データを前記受付センタへ送信し、前記受付センタは、各アンケート回答者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

【請求項34】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

窓口センタが、外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタへ転送し、

前記復号シャッフルセンタが、前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送し、前記窓口センタが、前記復号シャッフルセンタからデー

タリストが返送されてきた場合、該データリストを復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項35】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

窓口センタが、外部から受け取った暗号データリストを第1の復号シャッフルセンタに転送し、

前記第1の復号シャッフルセンタが、前記窓口センタから受け取った暗号データリストに対して、対応する公開情報を用いて順番入れ替え処理を行い、対応する復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタに返送し、

前記窓口センタが、前記第1の復号シャッフルセンタから返送されたデータリストを、第2の復号シャッフルセンタに送信し、

前記窓口センタが、最後の復号シャッフルセンタから返送されたデータリストを、復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項36】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

前記窓口センタが、外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第1番目の復号シャッフルセンタへ転送し、

前記各復号シャッフルセンタが、前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送し、

前記窓口センタが、処理順序が最後の復号シャッフルセンタ以外の復号シャッフルセンタからデータリストが返送されてきた場合、処理順序が前記データリストの返送元復号シャッフルセンタの次の復号シャッフルセンタに対して前記返送されてきたデータリストを暗号データリストとして転送し、処理順序が最後の復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項37】 請求項34、35または36記載の匿名復号方法において、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記窓口センタに報告することを特徴とする匿名復号方法。

【請求項38】 請求項34、35または36記載の匿名復号方法において、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記処理結果のデータリストに付して前記窓口センタに報告することを特徴とする匿名復号方法。

【請求項39】 請求項37または38記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証することを特徴とする匿名復号方法。

【請求項40】 請求項37または38記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証した後、前記復号シャッフルセンタから返送されてきたデータリストを暗号データリストとして、処理順序が次の復号シャッフルセンタに送信することを特徴とする匿名復号方法。

【請求項41】 請求項37、38、39または40記載の匿名復号方法において、

前記窓口センタは、復号結果リストに、全復号シャッフルセンタから報告された証明を付して出力することを特徴とする匿名復号方法。

【請求項42】 請求項34、35または36記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行うことを特徴とする匿名復号方法。

【請求項43】 請求項34、35または36記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付与することを特徴とする匿名復号方法。

【請求項44】 請求項34、35または36記載の匿名復号方法において、

同一処理対象に対する、互いに関連する公開情報、暗号データリスト、復号シャッフルセンタが所有する復号鍵に共通のセッションIDを付与し、

前記窓口センタは、或るセッションIDに対応する暗号データリストを復号シャッフルセンタへ転送する場合および復号シャッフルセンタから返送されてきた或るセッションIDの付与されたデータリストを暗号データリストとして復号シャッフルセンタへ転送する場合、前記暗号データリストに前記或るセッションIDを付与して復号シャッフルセンタへ転送し、

前記復号シャッフルセンタは、前記窓口センタから或るセッションIDの付与された暗号データリストが転送されてきた場合、前記或るセッションIDの付与されている公開情報を用いて順番入れ替え処理を行い、前記或るセッションIDの付与されている復号鍵を用いて部分復号を行い、その結果のデータリストに前記或るセッショ

10

20

30

40

50

ンIDを付与して前記窓口センタに返送することを特徴とする匿名復号方法。

【請求項45】 請求項34、35または36記載の匿名復号方法において、前記窓口センタが、セキュリティパラメータが入力されたとき、該セキュリティパラメータに基づいて共通公開情報を作成し、該作成した共通公開情報を全復号シャッフルセンタへ通知し、前記全復号シャッフルセンタが、前記窓口センタから通知された共通公開情報に基づいて、公開鍵および復号鍵を生成し、前記生成した公開鍵を前記窓口センタへ返送し、前記窓口センタが、前記全復号シャッフルセンタから公開鍵が返送されてきたとき、前記全復号シャッフルセンタからの公開鍵に基づいて暗号化用公開鍵を生成すると共に、該生成した暗号化用公開鍵と前記共通公開情報とを含んだ公開情報を公開することを特徴とする匿名復号方法。

【請求項46】 請求項45記載の匿名復号方法において、前記復号シャッフルセンタは、公開鍵を前記窓口センタへ返送するとき、正しく前記公開鍵を生成したことの証明を付与して前記窓口センタに返送することを特徴とする匿名復号方法。

【請求項47】 請求項46記載の匿名復号方法において、前記窓口センタは、公開鍵に付された証明が正しいことを検証することを特徴とする匿名復号方法。

【請求項48】 請求項46または47記載の匿名復号方法において、前記窓口センタは、公開鍵と、公開鍵に付与された証明を公開情報とともに公開することを特徴とする匿名復号方法。

【請求項49】 請求項45記載の匿名復号方法において、前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行うことを特徴とする匿名復号方法。

【請求項50】 請求項45記載の匿名復号方法において、前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付することを特徴とする匿名復号方法。

【請求項51】 請求項44記載の匿名復号方法において、前記窓口センタは、復号シャッフルセンタに対して暗号データリストを転送する際、前記セッションIDに加えて、自窓口センタに付与されている窓口センタID、転送先の復号シャッフルセンタに付与されている復号シャッフルセンタID及び自窓口センタの署名も付加することを特徴とする匿名復号方法。

【請求項52】 請求項44記載の匿名復号方法において、前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、前記セッションIDに加えて、自復号シャッフルセンタに付与されている復号シャッフルセンタID、前記窓口センタに付与されている窓口センタID及び自復号シャッフルセンタの署名も付加することを特徴とする匿名復号方法。

【請求項53】 請求項52記載の匿名復号方法において、前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、正しく順番入れ替え処理を行ったことの証明データ及び正しく部分復号処理を行ったことの証明データも付加することを特徴とする匿名復号方法。

【請求項54】 請求項41記載の匿名復号方法において、前記窓口センタが出力する情報が、自窓口センタに付与されている窓口センタID、外部から入力した暗号データリスト、該暗号データリストに対する復号結果、前記暗号データリストに付与されているセッションID、全復号シャッフルセンタから返送されてきた全データ及び窓口センタの署名を含むことを特徴とする匿名復号方法。

【請求項55】 請求項45記載の匿名復号方法において、前記窓口センタは、復号シャッフルセンタに対して共通公開情報およびセキュリティパラメータを通知する際、自窓口センタに付与されている窓口センタID、復号を行う全復号シャッフルセンタの復号シャッフルセンタID、セッションID及び窓口センタの署名を付加することを特徴とする匿名復号方法。

【請求項56】 請求項45または46記載の匿名復号方法において、復号シャッフルセンタは、窓口センタに返信する情報に、前記窓口センタに付与されている窓口センタID、セッションID、自復号シャッフルセンタの復号シャッフルセンタID及び自復号シャッフルセンタの署名を付加することを特徴とする匿名復号方法。

【請求項57】 請求項45記載の匿名復号方法において、前記窓口センタが公開する公開情報は、自窓口センタに付与されている窓口センタID、セッションID、セキュリティパラメータ、暗号化用公開鍵、全復号シャッフルセンタの復号シャッフルセンタID及び全復号シャッフルセンタが生成した公開鍵を含むことを特徴とする匿名復号方法。

【請求項58】 請求項37、38、42または46記載の匿名復号方法において、復号シャッフルセンタが行った証明は、第三者により検

10

20

30

40

50

証できるものであることを特徴とする匿名復号方法。

【請求項59】 請求項34、35または36記載の匿名復号方法において、前記復号シャッフルセンタは、順番入れ替え処理に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前計算したデータを用いて順番入れ替え処理を行うことを特徴とする匿名復号方法。

【請求項60】 請求項38記載の匿名復号方法において、前記復号シャッフルセンタは、順番入れ替え処理が正しいことを証明する証明データの生成に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前に計算したデータを用いて前記証明データを生成することを特徴とする匿名復号方法。

【請求項61】 請求項34乃至60記載の何れか1つの匿名復号方法において、投票管理センタが、各投票者から送られてくる、投票データを前記公開情報に基づいて暗号化した暗号化投票データを受け付け、その中から正当な投票者の正当な暗号化投票データを選別し、該選別した暗号化投票データを暗号データリストとして前記窓口センタに送信することを特徴とする匿名復号方法。

【請求項62】 請求項61記載の匿名復号方法において、前記各投票者は、正しく投票データを暗号化したことを証明する証明データを前記投票管理センタへ送信し、前記投票管理センタは、各投票者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項63】 請求項34乃至60記載の何れか1つの匿名復号方法において、入札管理センタが、各入札者から送られてくる、入札値を前記公開情報に基づいて暗号化した暗号化入札値を受け付け、その中から正当な入札者の正当な暗号化入札値を選別し、該選別した暗号化入札値を暗号化データリストとして前記窓口センタへ送信することを特徴とする匿名復号方法。

【請求項64】 請求項63記載の匿名復号方法において、前記各入札者は、正しく入札値を暗号化したことを証明する証明データを前記入札管理センタへ送信し、前記入札管理センタは、各入札者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項65】 請求項34乃至請求項60記載の何れか1つの匿名復号方法において、受付センタが、各アンケート回答者から送られてくる、アンケート回答を前記公開情報に基づいて暗号化した暗号化アンケート回答を受け付け、その中から正当なアンケート回答者の正当な暗号化アンケート回答を選別し、

該選別した暗号化アンケート回答を暗号化データリストとして前記窓口センタへ送信することを特徴とする匿名復号方法。

【請求項66】 請求項65記載の匿名復号方法において、前記アンケート回答者は、正しくアンケート回答を暗号化したことを証明する証明データを前記受付センタへ送信し、前記受付センタは、各アンケート回答者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項67】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムを構成する窓口センタ用コンピュータ及び復号シャッフルセンタ用コンピュータの内の窓口センタ用コンピュータに、

外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタ用コンピュータへ転送する処理、

前記復号シャッフルセンタ用コンピュータからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する処理を行わせ、

前記復号シャッフルセンタ用コンピュータに、前記窓口センタ用コンピュータから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタ用コンピュータが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタ用コンピュータへ返送する処理を行わせることを特徴とするプログラム。

【請求項68】 指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムを構成する窓口センタ用コンピュータ及び複数の復号シャッフルセンタ用コンピュータの内の窓口センタ用コンピュータに、

外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第一番目の復号シャッフルセンタ用コンピュータへ転送する処理、

処理順序が最後の復号シャッフルセンタ用コンピュータ以外の復号シャッフルセンタ用コンピュータからデータリストが返送されてきた場合、処理順序が前記データリストの返送元復号シャッフルセンタ用コンピュータの次の復号シャッフルセンタ用コンピュータに対して前記返送されてきたデータリストを暗号データリストとして転送する処理、

処理順序が最後の復号シャッフルセンタ用コンピュータ

からデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する処理を行わせ、前記各復号シャッフルセンタ用コンピュータに、前記窓口センタ用コンピュータから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタ用コンピュータが所有している復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタ用コンピュータへ返送する処理を行わせることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、匿名復号技術に関し、特に、暗号データとの対応を秘匿して復号結果を出力する匿名復号技術に関する。

【0002】

【従来の技術】従来のこの種の匿名復号システムとしては、例えば、特開平08-263575号公報に記載されているものが知られている。ここに記載されている匿名復号システムは、Mix-net方式に基づくものであり、図10に示すように、複数の復号シャッフルセンタ100-1～100-nと、インターネット等のネットワーク上に配置された外部からアクセス可能な電子掲示板200とから構成されている。

【0003】各復号シャッフルセンタ100-1～100-nは、部分復号手段101、シャッフル手段102、証明手段103を備えている。また、各復号シャッフルセンタ100-1～100-nは、別途定められたセキュリティパラメータに従って生成された暗号化用の公開鍵と、復号用の復号鍵とを保持している。また、図10に示した匿名復号システムでは、各復号シャッフルセンタ100-1～100-nの公開鍵を合成したものをデータ暗号化のための暗号化用公開鍵としている。

【0004】複数のセンダ（図示せず）が、暗号化用公開鍵を用いて暗号化した暗号データを電子掲示板200に書き込むと、処理順序が第1番目の復号シャッフルセンタ100-1が、上記複数のセンダが書き込んだ暗号データを暗号データリスト201として入力し、以下の処理を行う。

【0005】まず、部分復号手段101を用いて、暗号データリスト201に対する部分復号処理を行う。このとき、部分復号手段101は、復号シャッフルセンタ100-1が保持している復号鍵を使用する。次に、部分復号が行われた後の暗号データリストに対して、シャッフル手段102を使用して順番入れ替え処理を行う。その後、証明手段103を用いて、部分復号処理、順番入れ替え処理が正しく行われたことを証明する証明データを生成する。そして、最後に、部分復号処理、順番入れ替え処理を行った後の暗号データリスト（データリスト）と証明データとを含むデータ202-1を電子掲示

板200に書き込む。

【0006】電子掲示板200にデータ202-1が書き込まれると、処理順序が第2番目の復号シャッフルセンタ100-2が、データ202-1中のデータリストに対して、復号シャッフルセンタ100-1が行った処理と同様の処理を行い、データリスト及び証明データを含むデータ200-2を電子掲示板200に書き込む。

【0007】以下、同様の動作が最後の復号シャッフルセンタ100-nまで行われ、電子掲示板200に、復号結果リスト、証明データを含んだデータ203が書き込まれる。

【0008】

【発明が解決しようとする課題】上述した従来の匿名復号システムは、電子掲示板を利用しているため、次のような問題があった。つまり、各復号シャッフルセンタに部分復号処理、順番入れ替え処理を行わせたり、各センダに証明データの検証を行わせるためには、各復号シャッフルセンタ、各センダから電子掲示板を自由にリードできるようにしなければならない。更に、不正行為を防止するためには、電子掲示板に対するデータの書き込みを、正当なセンダ、復号シャッフルセンタからの正当なデータのみで制限しなければならない。このように、従来の匿名復号システムは、各復号シャッフルセンタ、各センダから電子掲示板を自由にリードできるようにし、且つ、電子掲示板に対するデータの書き込みを、正当なセンダ、復号シャッフルセンタからの正当なデータのみで制限しなければならないため、管理が複雑になるという問題があった。

【0009】また、匿名性の保護の観点から、実際の運用においては、匿名復号システムを構成する個々の復号シャッフルセンタは、すべて別々の組織によって運用されることが望ましい。しかし、別組織によって運用される場合、システムに必要な重要な各種パラメータ（利用者がメッセージを暗号化するための鍵など）を決定する初期設定作業が煩雑になるおそれがある。このため、重要なパラメータの決定経緯が不明確になるおそれがあり、ひいてはシステムの正常な運用を妨げる可能性がある。

【0010】そこで、本発明の目的は、複雑な管理処理を不要にすると共に、初期設定作業を容易且つ確実に実行できるようにすることにある。

【0011】

【課題を解決するための手段】本発明の匿名復号システムは、1個或いは複数の復号シャッフルセンタと、1個の窓口センタとから構成される。復号シャッフルセンタが1個の場合、窓口センタは、外部から入力された暗号データリストを復号シャッフルセンタへ転送し、復号シャッフルセンタから返送されてきたデータリスト（上記復号シャッフルセンタで暗号データリストに対して、部分復号処理、順番入れ替え処理を行ったもの）を復号

結果リストとして出力する。

【0012】また、復号シャッフルセンタが複数個の場合は、窓口センタは、外部から入力された暗号データリストを処理順序が第1番目の復号シャッフルセンタへ転送し、上記復号シャッフルセンタからデータリストが返送されてくると、それを暗号データリストとして処理順序が第2番目の復号シャッフルセンタへ転送する。以下、窓口センタは、或る復号シャッフルセンタからデータリストが返送されてくると、それを暗号データリストとして処理順序が次の復号シャッフルセンタへ転送するという処理を繰り返し行い、処理順序が最後の復号シャッフルセンタからデータリストが返送されてくると、それを復号結果リストとして出力する。このように、本発明の匿名復号システムによれば、窓口センタと復号シャッフルセンタ間でデータをやり取りするだけで、暗号データリストを復号することが可能になり、電子掲示板を使用した従来の匿名復号システムのような複雑な管理処理が不要になる。

【0013】また、本発明の匿名復号システムは、セキュリティパラメータが入力されたとき、窓口センタと各復号シャッフルセンタが共同して暗号化用公開鍵を含む公開情報を生成するようにしているので、初期設定作業を容易且つ確実に行うことが可能になる。

【0014】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して詳細に説明する。

【0015】図1を参照すると、本発明の第1の実施の形態としての匿名復号システムが示されている。この匿名復号システムは、ひとつの窓口センタ10と、複数個(m個)の復号シャッフルセンタ20-1~20-mとから構成されている。

【0016】窓口センタ10は、コンピュータによって構成されるものであり、外部からセキュリティパラメータが入力されたとき、各復号シャッフルセンタ20-1~20-mと共同して初期設定処理を行い、暗号化用公開鍵等を含む公開情報を生成する機能や、外部から上記暗号化用公開鍵によって暗号化された暗号データを複数含む暗号データリストが入力されたとき、復号シャッフルセンタ20-1~20-mを所定の順序(例えば、外部から指示された順序)で順次使用して上記暗号データリストを復号する機能等を有する。

【0017】このような機能を有する窓口センタ10は、例えば、図2に示すように、窓口側初期設定手段11と、復号制御手段12とを備えている。

【0018】窓口側初期設定手段11は、外部からセキュリティパラメータが入力されたとき、各復号シャッフルセンタ20-1~20-mと共同して暗号化用公開鍵等を含む公開情報を生成し公開する機能等を有する。復号制御手段12は、暗号データリストが入力されたとき、復号シャッフルセンタ20-1~20-mを順次使

用して暗号データリストを復号し、復号結果である復号結果リストを公開する機能等を有する。

【0019】窓口センタ10に接続されている記録媒体K10は、ディスク、半導体メモリ、その他の記録媒体であり、コンピュータからなる窓口センタ10を匿名復号システムの一部として機能させるためのプログラムが記録されている。このプログラムは、コンピュータからなる窓口センタ10によって読み取られ、その動作を制御することで、窓口センタ10上に窓口側初期設定手段11、復号制御手段12を実現する。

【0020】復号シャッフルセンタ20-1~20-mは、コンピュータによって構成されるものであり、窓口センタ10と例えば専用回線を介して接続されている。各復号シャッフルセンタ20-1~20-mは、窓口センタ10と共同して初期設定処理を行う機能や、窓口センタ10から送られてきた暗号データリストに対して、順番入れ替え処理、部分復号処理を行い、その処理結果を窓口センタ10に返送する機能等を有する。

【0021】このような機能を有する復号シャッフルセンタ20-j(1≦j≦m)は、例えば、図3に示すように、シャッフル側初期設定手段21と、シャッフル手段22と、部分復号手段23と、証明手段24とを備えている。

【0022】シャッフル側初期設定手段21は、窓口側初期設定手段11と共同して初期設定処理を行う機能を有する。この初期設定処理に於いて、シャッフル側初期設定手段21は、公開鍵、復号鍵の生成を行う。シャッフル手段22は、窓口センタ10から送られてきた暗号データリストに対して、順番入れ替え処理を行う機能を有する。部分復号手段23は、シャッフル手段22が順番入れ替え処理を行った後の暗号データリストに対して、部分復号処理を行う機能を有する。証明手段24は、シャッフル手段22の処理が正しいことを証明する証明データを生成する機能や、部分復号手段23の処理が正しいことを証明する証明データを生成する機能を有する。

【0023】復号シャッフルセンタ20-jに接続されている記録媒体K20-jは、ディスク、半導体メモリ、その他の記録媒体であり、コンピュータからなる復号シャッフルセンタ20-jを匿名復号システムの一部として機能させるためのプログラムが記録されている。このプログラムは、コンピュータからなる復号シャッフルセンタ20-jによって読み取られ、その動作を制御することで、復号シャッフルセンタ20-j上にシャッフル側初期設定手段21、シャッフル手段22、部分復号手段23、証明手段24を実現する。

【0024】次に、本実施の形態の動作について詳細に説明する。

【0025】＜初期設定処理＞まず、初期設定処理について説明する。

10

20

30

40

50

【0026】外部からセッションIDの付加されたセキュリティパラメータ(pL, qL, t)が入力されると、窓口センタ10内の窓口側初期設定手段11は、共通公開情報(p, q, g)を生成する(図4, A1)。ここで、p, qは、エルガマル暗号のパラメータであり、或る整数kにより $p = kq + 1$ という関係にある2素数である。gは、法pにおける位数qの部分群を生成する生成元である。また、pL, qLは、素数p, qの長さであり、tは後述する順番入れ替え処理が正しいことを証明する証明データの生成時及び上記証明データの検証時に使用する繰り返し回数である。また、セッションIDは、処理対象を特定するための識別子であり、処理対象とは、例えば、県知事選挙、市議会議員選挙等である。

【0027】その後、窓口側初期設定手段11は、共通公開情報(p, q, g)を含んだ公開鍵生成依頼文を作成し、それに窓口センタ10のデジタル署名およびセッションIDを付して全復号シャッフルセンタ20-1~20-mへ転送する(A2)。

【0028】各復号シャッフルセンタ20-1~20-m内のシャッフル側初期設定手段21は、公開鍵生成依頼文に付されているデジタル署名を検証することにより、相手認証を行う(A3)。そして、署名が正しくなければ、例えば処理終了とする。これに対して、署名が正しければ、共通公開情報(p, q, g)の正当性を確認する。すなわち、(p, q, g)が第【0026】段落に記載されている関係を満たすかどうか調べる。正当性を確認できなければ、例えば処理終了とする。これに対して正当性を確認できれば、共通公開情報(p, q, g)に基づいて、公開鍵および復号鍵(秘密鍵)を生成し、それらを自復号シャッフルセンタ内に、セッションIDと対応付けて保持する(A4)。例えば、処理順序が第j番目の復号シャッフルセンタ20-jにおいては、無作為に $x_j \bmod q$ を選び、それを復号鍵とする。また、自復号シャッフルセンタ20-jの公開鍵 y_j を

$$y_j = g^{x_j} \bmod p$$

により生成する。

【0029】その後、各復号シャッフルセンタ20-1~20-m内のシャッフル側初期設定手段21は、ステップA4で生成した公開鍵に対して復号鍵を知っていることの証明データを生成する(A5)。例えば、処理順序が第j番目の復号シャッフルセンタ20-j内のシャッフル側初期設定手段21では、公開鍵 y_j に対して復号鍵 x_j を知っていることの証明データ y'_j , r_j を

$$y'_j = g^{x_j} \bmod p$$

$$c_j = \text{Hash}(p, q, g, y_j, y'_j)$$

$$r_j = c_j x_j + \beta_j \bmod q$$

により生成する。ここで、Hashは安全なハッシュ関

数、 β_j は乱数である。

【0030】ステップA5の処理が終了すると、各復号シャッフルセンタ20-1~20-m内のシャッフル側初期設定手段21は、ステップA4で生成した公開鍵及びステップA5で生成した証明データを含む公開鍵登録依頼文を作成し、それに自復号シャッフルセンタのデジタル署名及びセッションIDを付して窓口センタ10へ返送する(A6)。

【0031】窓口センタ10内の窓口側初期設定手段11は、各復号シャッフルセンタ20-1~20-mから返送されてきた公開鍵登録依頼文に付されているデジタル署名を検証することにより相手認証を行い(A7)、更に、各復号シャッフルセンタ20-1~20-mから返送されてきた公開鍵の正当性を

$$c_j = \text{Hash}(p, q, g, y_j, y'_j)$$

$$g^{r_j} y_j^{-c_j} = y'_j \bmod p$$

$$y_j^q = 1 \bmod p$$

$$y_j \neq 1 \bmod p$$

により検証する(A8)。

【0032】そして、復号シャッフルセンタ20-1~20-mから返送されてきた全ての公開鍵登録依頼文が、ステップA7, A8の検証を通った場合は、各復号シャッフルセンタ20-1~20-mから返送されてきた公開鍵 $y_1 \sim y_m$ を、

$$Y = \prod_{j=1}^m y_j \bmod p$$

により合成し、システム利用者がデータを暗号化の際に使用する暗号化用公開鍵Yを生成する(A9)。

【0033】その後、窓口側初期設定手段11は、暗号化用公開鍵Y, 各復号シャッフルセンタ20-1~20-mの公開鍵 $y_1 \sim y_m$, 共通公開情報(p, q, g)及び各復号シャッフルセンタ20-1~20-mの復号シャッフルセンタID(どのような組織が復号を担当しているのかをシステム利用者に知らせるため)を含む公開情報を生成し、この公開情報をセッションIDと対応付けて公開する(A10)。以上が初期設定処理である。

【0034】次に、復号処理について説明する。

【0035】窓口センタ10内の復号制御手段12には、外部からn個の暗号データを含んだ暗号データリスト $\{(G_i, M_i)\}_{(i=1,2,\dots,n)}$ が入力される。この暗号データリストには、それがどの処理対象に関連するものであるのかを特定するためのセッションIDが付与されている。

【0036】暗号データ (G_i, M_i) は、データ m_i に対応する暗号データであり、

$$(G_i, M_i) = (g^{r_i}, m_i Y^{r_i}) \bmod p$$

10

20

30

40

50

により得られたものである。ここで、データ m_i は、位数が q になるように選ばれているものとする。また、 r_i は、データ m_i に対して任意に選んだ乱数である。

【0037】窓口センタ10内の復号制御手段12は、暗号データリスト $\{(G_i, M_i)\}_{(i=1,2,\dots,n)}$ が入力されると、 G_i, M_i の位数が q であることを全ての i について確認したのち、それに窓口センタ10のデジタル署名、セッションIDを付して処理順序が第1番目の復号シャッフルセンタ20-1に転送する(図5, B1, B2)。尚、処理順序が第 j 番目の復号シャッフルセンタ20-jへ転送する暗号データリストは、 $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ と記すものとする。

【0038】復号シャッフルセンタ20-1は、暗号データリスト $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ に付されているデジタル署名を検証することにより相手認証を行う(図6, C1)。そして、デジタル署名が正しいものであれば、シャッフル手段22, 部分復号手段23を用いて上記暗号データリストに対して順番入れ替え処理, 部分復号処理を行い、処理結果であるデータリストを得る(C2, C3)。尚、順番入れ替え処理, 部分復号処理については、後で詳細に説明する。その後、証明手段24を用いてシャッフル手段22, 部分復号手段23が行った処理が正しいことを示す証明データを生成し(C4)、データリスト, 証明データにデジタル署名およびセッションIDを付して窓口センタ10へ返送する(C5)。ここで、証明データは、データリストに付加して窓口センタ10へ返送しても良いし、先にデータリストだけを返送し、後から証明データを個別で返送するようにしても良い。尚、証明データの生成方法については、後で詳細に説明する。

【0039】窓口センタ10内の復号制御手段12は、復号シャッフルセンタ20-1からデジタル署名、セッションIDの付されたデータリスト, 証明データが返送されてくると、デジタル署名に基づいて、相手認証を行うと共に、証明データを検証する(図5, B3)。尚、証明データの検証方法については、後で詳細に説明する。そして、デジタル署名, 証明データが正しいものである場合は、処理順序が第2番目の復号シャッフルセンタ20-2に、処理順序が第1番目の復号シャッフル

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\} = \{(G_{\pi(i)}^{(j)}, M_{\pi(i)}^{(j)})\} (i=1, 2, \dots, n)$$

が成り立っている。

【0045】シャッフル処理が終了すると、再暗号処理を行う。ここで、再暗号とは、暗号化されたデータの内容を変えずに暗号データの「見かけ」を変えることである。単に位置を変えただけでは、暗号データのビットパターンから暗号データを追跡することが可能であるため、再暗号処理が必要になる。

【0046】そこで、処理順序が第 j 番目の復号シャッフルセンタ20-j内のシャッフル手段22は、自復号

*ルセンタ20-1から返送されてきたデータリストを暗号データリストとして転送する(B4~B6)。その際、復号制御手段12は、暗号データリストに、セッションIDを付加する。

【0040】復号シャッフルセンタ20-2でも、復号シャッフルセンタ20-1と同様の処理が行われ(図6, C1~C5)、窓口センタ10にデジタル署名, セッションIDの付されたデータリスト, 証明データが返送される。

【0041】これにより、窓口センタ10内の復号制御手段12は、前述した処理と同様の処理を行う(図5, B3~B6)。以上の処理が繰り返し行われ、処理順序が最後の復号シャッフルセンタ20-mからデジタル署名, セッションIDの付されたデータリスト, 証明データが返却されると、復号制御手段20は、上記データリストを復号結果リストとして公開する(B7)。その際、各復号シャッフルセンタ20-1~20-mから送られてきた各証明データ, セッションID, 窓口センタ10の窓口センタID, 復号シャッフルセンタ20-1~20-mの復号シャッフルセンタIDも公開する。

【0042】以下に、シャッフル手段22が行う順番入れ替え処理, 部分復号手段23が行う部分復号処理, 証明手段24が行う証明データ生成処理, 復号制御手段12が行う検証処理について詳しく説明する。

【0043】＜順番入れ替え処理＞処理順序が第 j 番目の復号シャッフルセンタ20-j内のシャッフル手段22が行う順番入れ替え処理について説明する。順番入れ替え処理は、以下に述べるシャッフル処理と再暗号処理とからなる。

【0044】シャッフル手段22は、先ず、シャッフル処理を行う。シャッフル処理においては、窓口センタ10から送られてきた暗号データリスト $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ 中の暗号データ $(G_i^{(j)}, M_i^{(j)})_{(i=1,2,\dots,n)}$ に対して、ランダムに置換写像 $\pi^{(j)}$ を決定し、それに基づいて $(G_i^{(j)}, M_i^{(j)})_{(i=1,2,\dots,n)}$ の順番を入れ替え、新たに、

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\}_{(i=1,2,\dots,n)}$$

を得る。以上がシャッフル処理である。このとき、

シャッフルセンタ以降の復号シャッフルセンタの公開鍵を合成して、

$$Y_j = \prod_{t=j}^m y_t \bmod p$$

を求める。そして、シャッフル処理された

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\}_{(i=1,2,\dots,n)}$$

に対して、乱数 $s^{(j)} \bmod q$ を発生させて、

$$\begin{aligned} G_i^{(j)} &= \bar{G}_i^{(j)} \cdot g^{s_i^{(j)}} \bmod p \\ M_i^{(j)} &= \bar{M}_i^{(j)} \cdot Y_j^{s_i^{(j)}} \bmod p \end{aligned}$$

により、 $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ を求める。

【0047】尚、 Y_j や、乱数 $s_i^{(j)}$ の発生、および $g^{s_i^{(j)}}, Y_j^{s_i^{(j)}}$

の計算は、暗号データリストを受け取る前に事前計算しておくことができる。事前計算した値を保存しておけば、各データ成分に対して、この再暗号処理は、1回の乗算のみで実現できる。

【0048】＜部分復号処理＞次に、復号シャッフルセンタ20-j内の部分復号手段23が行う部分復号処理について説明する。

【0049】部分復号手段23は、シャッフル手段22が順番入れ替え処理を行った $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ に対して、自復号シャッフルセンタ20-jが所有している復号鍵 x_j (暗号データリストに付されているセッションIDに対応する復号鍵)を用いて、

$$\begin{aligned} M_i^{(j)} &= M_i^{(j)} / (G_i^{(j)})^{x_j} \bmod p \\ G_i^{(j)} &= G_i^{(j)} \end{aligned}$$

を計算する。そして、

$$(G_i^{(j)}, M_i^{(j)})_{(i=1,2,\dots,n)}$$

をデータリストとして窓口センタ10へ返送する。*30

・ $c[u] = 0$ のとき、 $\alpha_u = \pi'_u$ 及び $\beta_{(u,v)} = s'_{(u,v)}$ とおく。

・ $c[u] = 1$ のとき、 $\alpha_u = \pi^{-1} \alpha \pi'_u$ 及び $\beta_{(u,v)} = s'_{(u,v)} - s_{(\pi^{-1} \alpha \pi'_u(u))}$ とおく。

とおく。証明データは、 $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ 、 $\{A_{(u,v)}, B_{(u,v)}\}$ 、 $\{\alpha_u\}$ 、 $\{\beta_{(u,v)}\}$ となる。

【0053】尚、置換写像 π'_u や乱数 $\{s'_{(u,v)}\}$ の発生および

$$g^{s'_{(u,v)}}, Y_j^{s'_{(u,v)}}$$

の計算は、暗号データリストを受け取る前に事前計算しておくことができる。事前計算をした値を保存しておけば、処理時間を短縮することが可能になる。

【0054】次に、上記した $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ に対して、自分の公開鍵 y に対する秘密鍵 x を用いて正しく計算した $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ を窓口センタ10に送ったことを秘密鍵 x を漏らさずに証明する証明データの生成方法について説明する。

【0055】1. 乱数 $r \bmod q$ を生成する。

*【0050】＜証明データ生成処理＞次に、証明手段24が行う証明データ生成処理について説明する。尚、以下の説明においては、復号シャッフルセンタを特定する (j) の表記を省略する。

【0051】まず、シャッフル手段22がデータリスト $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ に対して、置換写像 π を用いてシャッフル処理を行い、公開鍵情報 (p, q, g, Y_j) と乱数列 $\{s_i\}_{(i=1,2,\dots,n)}$ を用いて $\{(G_i^{(j)}, M_i^{(j)})\}_{(i=1,2,\dots,n)}$ を生成したことを、置換写像 π と乱数列 $\{s_i\}$ を秘密にして証明する証明データの生成方法について説明する。尚、以下の説明において、 t はセキュリティパラメータ (繰り返し回数) である。

【0052】1. t 個のランダムな置換写像 π'_u と、 $t \times n$ 個の乱数 $\{s'_{(u,v)}\}$ を発生させ、

$$A_{u,v} = G_{\pi'_u(v)} \cdot g^{s'_{(u,v)}} \bmod p$$

$$B_{u,v} = M_{\pi'_u(v)} \cdot Y_j^{s'_{(u,v)}} \bmod p$$

を $u = 1, 2, \dots, t, v = 1, 2, \dots, n$ に関して計算する。2.

$$\begin{aligned} c &= Hash(p||q||g||Y_j||\{(G_i, M_i)\}_{(i=1,\dots,n)}|| \\ &\quad \{(G'_i, M'_i)\}_{(i=1,\dots,n)}|| \\ &\quad \{(A_{(u,v)}, B_{(u,v)})\}_{(u=1,\dots,t,v=1,\dots,n)}) \end{aligned}$$

を計算する。ここで、 $||$ は連結を示す。3. c の u 番目 ($u = 1, 2, \dots, t$) のビットを $c[u]$ とすると、

2.

$$\begin{aligned} c &= Hash(p||q||g||Y_j||\{G_i\}_{(i=1,\dots,n)}|| \\ &\quad \{(M'_i/M_i)\}_{(i=1,\dots,n)}||g^r||\{G'_i\}_{(i=1,\dots,n)}) \end{aligned}$$

とおく。

3. $\alpha = r - c \times \bmod q$ とおく。

40 以上のようにして求めた c, α が証明データとなる。

【0056】＜検証処理＞次に、復号制御手段12が行う検証処理について説明する。まず、シャッフル手段22の処理が正しいことを証明する証明データの検証について説明する。

【0057】1. 公開された情報及び証明データから

$$\begin{aligned} c &= Hash(p||q||g||Y_j||\{(G_i, M_i)\}_{(i=1,\dots,n)}|| \\ &\quad \{(G'_i, M'_i)\}_{(i=1,\dots,n)}|| \\ &\quad \{(A_{(u,v)}, B_{(u,v)})\}_{(u=1,\dots,t,v=1,\dots,n)}) \end{aligned}$$

を計算する。

2. c の u 番目 ($u = 1, 2, \dots, t$) のビットを c

$[u]$ とすると、 $\cdot c[u] = 0$ のとき、

$$A_{u,v} = G_{\alpha_u(v)} \cdot g^{\beta(u,v)} \bmod p$$

$$B_{u,v} = M_{\alpha_u(v)} \cdot Y_j^{\beta(u,v)} \bmod p$$

が成り立つことを確認する。

$\cdot c[u] = 1$ のとき、

$$A_{u,v} = G'_{\alpha_u(v)} \cdot g^{\beta(u,v)} \bmod p$$

$$B_{u,v} = M'_{\alpha_u(v)} \cdot Y_j^{\beta(u,v)} \bmod p$$

が成り立つことを確認する。

3. G'_i, M'_i の位数が q であることを確認する。全てが確認できれば、証明データは正しいとみなす。

【0058】次に、部分復号手段23が行った処理が正しいことを証明する証明データの検証について説明する。

【0059】1. 全ての i について $G'_i = G''_i$ であることを確認する。

【0060】2.

$$c = \text{Hash}(p||q||g||y||\{G'_i\}_{i=1,\dots,n})||$$

$$\{(M'_i/M_i^p)\}_{i=1,\dots,n}||g^a \cdot y^c||$$

$$\{G_i^a \cdot (M'_i/M_i^p)^c\}_{i=1,\dots,n})$$

が成り立つことを確認する。

【0061】3. 全ての i について $M''_i = 1 \bmod p$ であることを確認する。全てが確認できれば、証明データは正しいとみなす。実際には、シャッフル証明と復号証明は一度に行われる。従って、復号結果として与えられている $\{G''_i\}_{i=1,2,\dots,n}$ に対して $G'_i = G''_i$ となるはずの $\{G'_i\}_{i=1,2,\dots,n}$ を送る必要はない。従って、実装では、シャッフル証明時に $\{M'_i\}_{i=1,2,\dots,n}$ のみを送るようにする。

【0062】尚、以上の動作説明では説明を省略したが、窓口センタと復号シャッフルセンタとでデータをやり取りする場合には、データに転送先の窓口センタ、復号シャッフルセンタのID及び転送元の窓口センタ、復号シャッフルセンタのIDを付加するものとする。例えば、窓口センタ10から復号シャッフルセンタ20-1へデータを転送する場合には、復号シャッフルセンタ20-1、窓口センタのIDをそれぞれ転送先、転送元として付加する。また、例えば、窓口センタ10から全ての復号シャッフルセンタ20-1~20-mへデータを転送する場合には、全復号シャッフルセンタ20-1~20-mのID、窓口センタ10のIDをそれぞれ転送先、転送元として付加する。

【0063】次に、図7を参照して本発明の第2の実施の形態について説明する。本実施の形態は、無記名電子投票を行う際に利用すると好適なものであり、図1に示

した匿名復号システムが備えている構成に加え、投票管理センタ30が追加されている。

【0064】投票管理センタ30には、有権者名簿と、セキュリティパラメータと、選挙の投票期間と、セッションIDとが入力される。投票管理センタ30は、上記セキュリティパラメータに上記セッションIDを付加し、窓口センタ10へ転送する。

【0065】窓口センタ10は、投票管理センタ30からセッションIDの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ20-1~20-mと共同して前述した初期設定処理(図4参照)を行い、得られた公開情報(公開鍵 Y 、共通公開情報 p, q, g 等を含む)を公開する。投票管理センタ30は、その公開情報がセキュリティパラメータに従って正当なものであることを確認し、各投票者に通知する。

【0066】投票期間が始まると投票者は、自分の投票データを公開情報を基に暗号化し、投票者のデジタル署名を付加して投票管理センタ30に送付する。ここで、第 i ($= 1, 2, \dots, n$) 番目の投票者は、公開された公開鍵 Y 及び共通公開情報 (p, q, g) を用いて投票内容 m_i を以下のように暗号化する。尚、ここで、投票内容は位数が q になるように選ばれているものとする。

【0067】まず、投票者は、任意の乱数 $r_i \bmod q$ を選ぶ。次に、

$$(G_i, M_i) = (g^{r_i}, m_i Y^{r_i}) \bmod p$$

により得られた (G_i, M_i) を暗号投票データとする。

この暗号投票データに自身のデジタル署名を付して投票センタ30へ送付する。

【0068】ここで、投票者が正しく m_i を知って暗号投票データを作成したことの証明を施すことができる。例えば、第 i 番目の投票者は、乱数 γ を発生させ、

$$\alpha_i = g^{\gamma} \bmod p$$

$$c_i = \text{Hash}(p, q, g, G_i, \alpha_i)$$

$$t_i = c_i r_i + \gamma_i \bmod q$$

により、証明データ α_i, t_i を生成する。この証明は、

$$c_i = \text{Hash}(p, q, g, G_i, \alpha_i)$$

$$g^{t_i} G_i^{-c_i} = \alpha_i \bmod p$$

により検証することができる。

【0069】或いは、第 i 番目の投票者は、乱数 γ を発生させ、

$$\alpha_i = g^{\gamma} \bmod p$$

$$c_i = \text{Hash}(p, q, g, G_i, \alpha_i)$$

$$t_i = \gamma_i - c_i r_i \bmod q$$

により、証明データ α_i, t_i を生成しても良い。この証

明は、

$$\begin{aligned} c_i &= \text{Hash}(p, q, g, G_i, \alpha_i) \\ g^{t_i} G_i^{c_i} &= \alpha_i \bmod p \end{aligned}$$

により検証することができる。

【0070】投票管理センタ30は、署名を検証し、有権者名簿をもとに投票者の投票権を確認し、二重投票をチェックした後、投票を受け付ける。尚、証明データが付加されている場合は、更に、証明データを検証した後、投票を受け付ける。投票期間が終わると投票の受け付けを終了し、受け付けた暗号投票データを暗号データリストとして匿名復号システムの窓口センタ10にデジタル署名付きで送信する。窓口センタ10は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを投票管理センタ30に返送する。

【0071】投票管理センタ30は、受け取った復号結果を復号後の投票データとして集計し、発表する。

【0072】次に、図8を参照して本発明の第3の実施の形態について説明する。本実施の形態は、匿名電子入札を行う際に利用すると好適なものであり、図1に示した匿名復号システムが備えている構成に加え、入札管理センタ40が追加されている。

【0073】入札管理センタ40には、入札者名簿と、セキュリティパラメータと、入札期間と、セッションIDとが入力される。入札管理センタ40は、上記セキュリティパラメータに上記セッションIDを付加し、窓口センタ10へ転送する。

【0074】窓口センタ10は、入札管理センタ40からセッションIDの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ20-1～20-mと共同して前述した初期設定処理（図4参照）を行い、得られた公開情報（公開鍵Y、共通公開情報p, q, g等を含む）を公開する。入札管理センタ40は、その公開情報がセキュリティパラメータに従って正当なものであることを確認し、各入札者に通知する。

【0075】入札期間が始まると入札者は、自分の入札値を公開情報を基に暗号化し、入札者のデジタル署名を付加して入札管理センタ40に送付する。その際、自分の入札値を知っていることを証明する証明データ（第2の実施の形態で説明した証明データと同様の証明データ）を送付するようにしても良い。

【0076】入札管理センタ40は、署名を検証し、入札者名簿をもとに入札者の入札権を確認し、二重の入札がないかをチェックした後、入札を受け付ける。尚、証明データも送付される場合には、証明データを検証した後、入札を受け付ける。入札期間が終わると入札の受け付けを終了し、受け付けた暗号入札値を暗号データリストとして匿名復号システムの窓口センタ10に送信す

る。窓口センタ10は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを入札管理センタ40に返送する。

【0077】入札管理センタ40は、受け取った復号結果を復号後の入札値として発表する。

【0078】次に、図9を参照して本発明の第4の実施の形態について説明する。本実施の形態は、匿名電子アンケートを行う際に利用すると好適なものであり、図1に示した匿名復号システムが備えている構成に加え、受付センタ50が追加されている。

【0079】受付センタ50には、回答者名簿と、セキュリティパラメータと、アンケート期間と、セッションIDとが入力される。受付センタ50は、上記セキュリティパラメータに上記セッションIDを付加し、窓口センタ10へ転送する。

【0080】窓口センタ10は、受付センタ50からセッションIDの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ20-1～20-mと共同して前述した初期設定処理（図4参照）を行い、得られた公開情報（公開鍵Y、共通公開情報p, q, g等を含む）を公開する。受付センタ50は、その公開情報がセキュリティパラメータに従って正当なものであることを確認し、各アンケート回答者に通知する。

【0081】アンケート期間が始まるとアンケート回答者は、自分のアンケート回答を公開情報を基に暗号化し、アンケート回答者のデジタル署名を付加して受付センタ50に送付する。その際、自分のアンケート回答を知っていることを証明する証明データ（第2の実施の形態で説明した証明データと同様の証明データ）を送付するようにしても良い。

【0082】受付センタ50は、署名を検証し、回答者名簿をもとに回答者の回答権を確認し、二重回答がないかをチェックした後、アンケート回答を受け付ける。尚、証明データも送付される場合には、証明データを検証した後、アンケート回答を受け付ける。アンケート期間が終わるとアンケート回答の受け付けを終了し、受け付けた暗号アンケート回答を暗号データリストとして匿名復号システムの窓口センタ10に送信する。窓口センタ10は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを受付センタ50に返送する。

【0083】受付センタ50は、受け取った復号結果を復号後のアンケート回答として発表する。

【0084】なお、本実施例で述べた以外にも、センタ或いは第三者が、公開されている情報やデータの正当性を適宜検証することが考えられる。また、証明方法に関する数式は一例であり、式を変更して同様の効果がえられることは同業者は容易に想定できることである。

【0085】

【発明の効果】以上説明したように、本発明によれば、窓口センタと復号シャッフルセンタとの間でデータをやり取りするだけで暗号データリストを復号することが可能になり、電子掲示板を用いた従来の匿名復号システムのような複雑な管理処理が不要になるという効果がある。

【0086】また、本発明では、外部から入力されたセキュリティパラメータに基づいて、窓口センタと復号シャッフルセンタが共同して暗号化用公開鍵を含む公開情報を生成するので、初期設定操作を容易且つ確実に行うことが可能になる効果がある。

【0087】また、復号鍵という重要な秘密を管理する復号シャッフルセンタが、不特定多数からアクセスされる電子掲示板と直接接続する必要が生じないので、セキュリティ面の効果が顕著である。更に、復号シャッフルセンタの構成を、復号鍵に関わる処理と窓口センタとの通信機能のみに集約できるので、コンパクトに実現できるという効果がある。また、窓口センタと復号シャッフルセンタで、セッション管理機能と復号鍵管理機能をそれぞれ分担したので、1度きりの匿名復号のみならず、複数回の匿名復号処理や、電子投票、電子入札、電子アンケートなど、すべて高いセキュリティでサービスを実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の構成例を示すブロック図である。

【図2】窓口センタ10の構成例を示すブロック図である。

【図3】復号シャッフルセンタ20-jの構成例を示すブロック図である。

【図4】初期設定時の処理例を示す流れ図である。

【図5】復号制御手段12の処理例を示す流れ図である。

* 【図6】復号シャッフルセンタ20-1~20-mの処理例を示す流れ図である。

【図7】本発明の第2の実施の形態の構成例を示すブロック図である。

【図8】本発明の第3の実施の形態の構成例を示すブロック図である。

【図9】本発明の第4の実施の形態の構成例を示すブロック図である。

【図10】従来の技術を説明するためのブロック図である。

【符号の説明】

10…窓口センタ

11…窓口側初期設定手段

12…復号制御手段

K10…記録媒体

20-1~20-m…復号シャッフルセンタ

21…シャッフル側初期設定手段

22…シャッフル手段

23…部分復号手段

24…証明手段

K20-1~K20-m…記録媒体

30…投票管理センタ

40…入札管理センタ

50…受付センタ

100-1~100-n…復号シャッフルセンタ

101…部分復号手段

102…シャッフル手段

103…証明手段

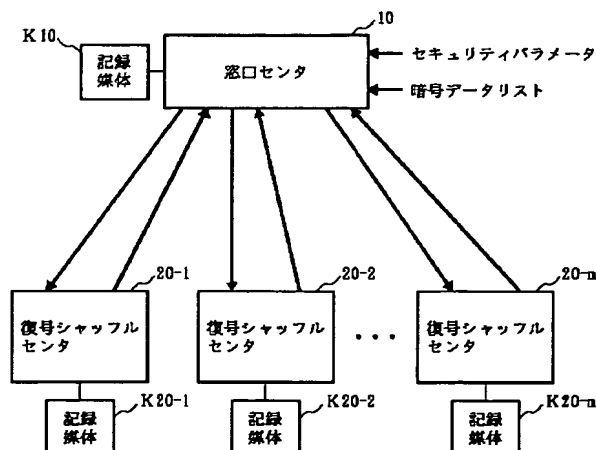
200…電子掲示板

201…暗号データリスト

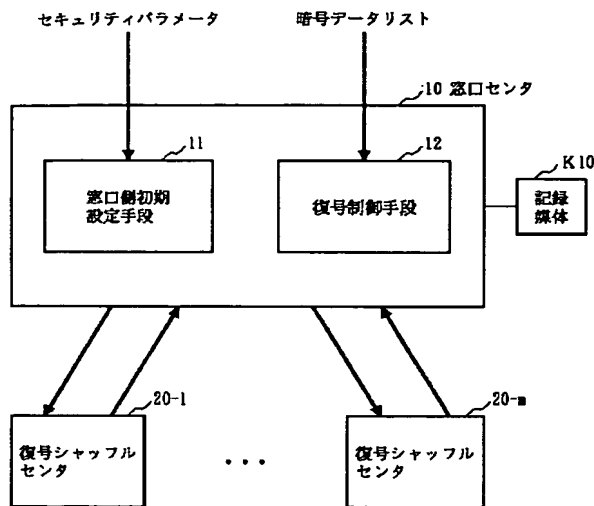
202-1, 202-2…処理された暗号データリスト, 証明データを含むデータ

* 203…復号結果リスト, 証明データを含むデータ

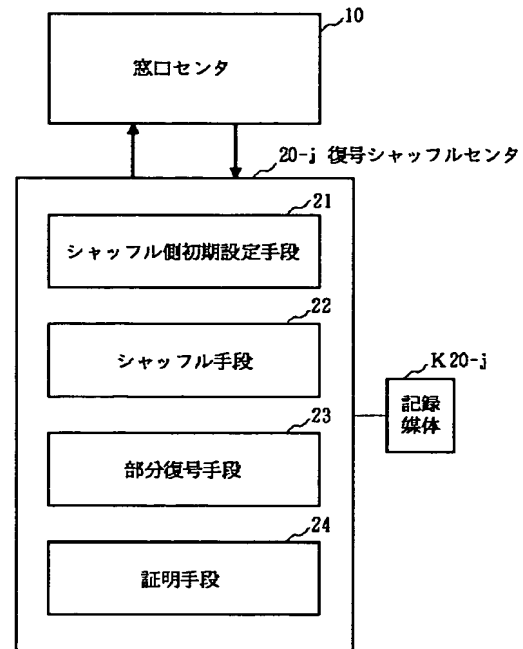
【図1】



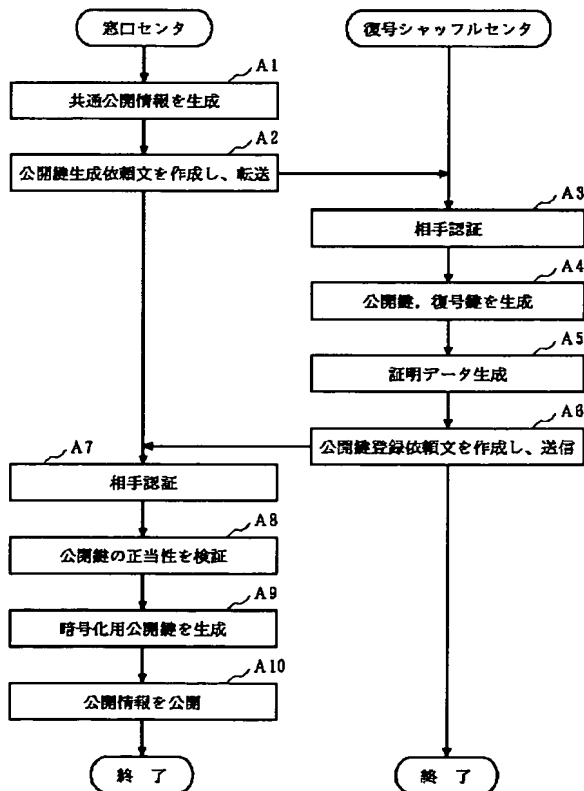
【図2】



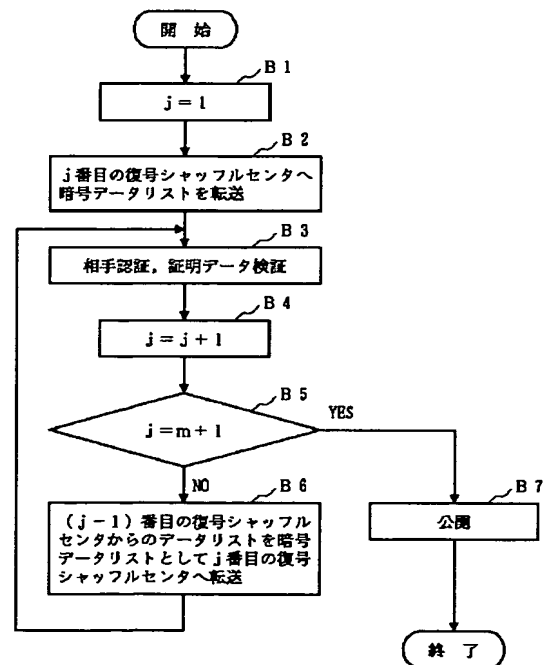
【図3】



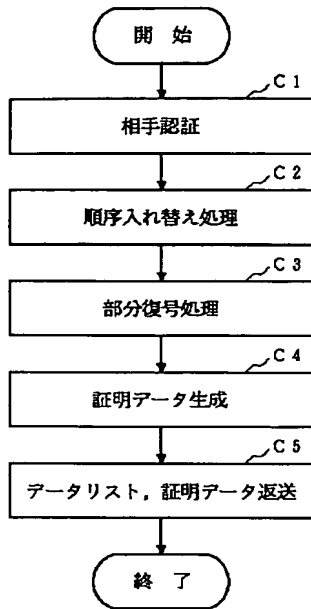
【図4】



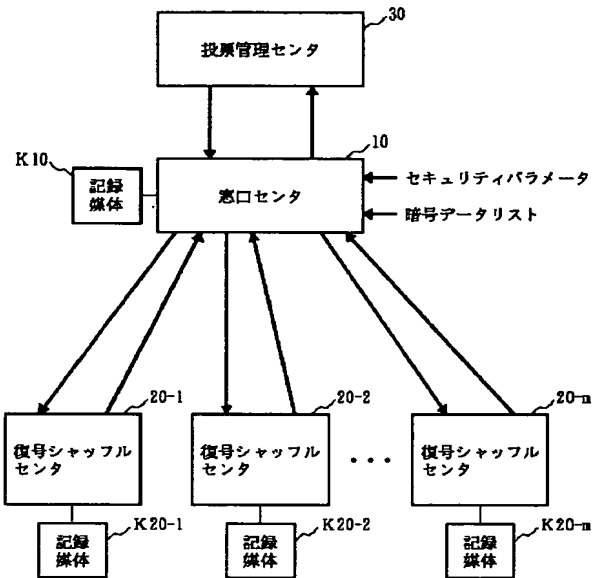
【図5】



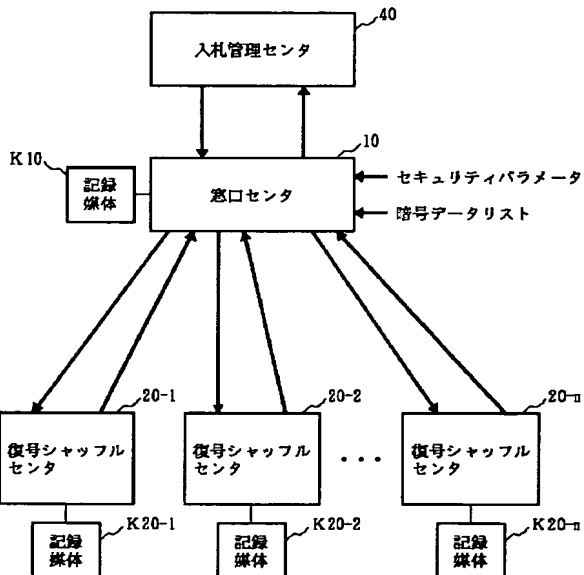
【図6】



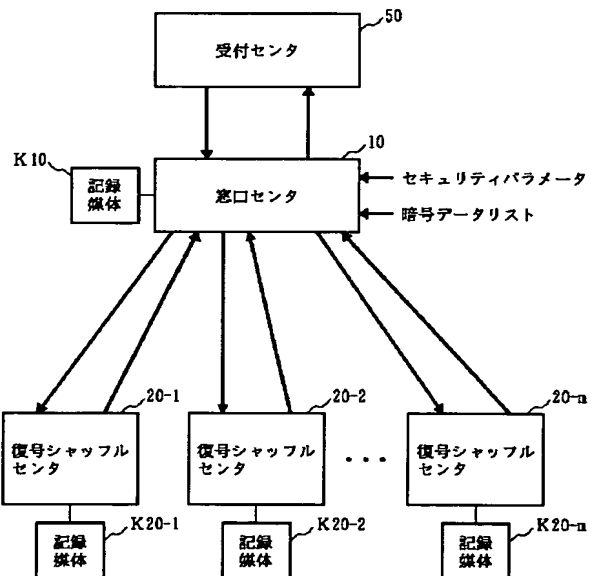
【図7】



【図8】



【図9】



【図10】

